Simulated Phishing Attack Using Zphisher in a Controlled Lab

Author: Onaopemipo Olugbemiro

Date: July 2025

Tools used: Kali Linux, Zipisher

Environment: Virtual Box

Objective

The purpose of this lab exercise was to simulate a phishing attack in a controlled and ethical environment using Zphisher, with the aim of understanding the techniques attackers use in social engineering to trick users into revealing sensitive information.

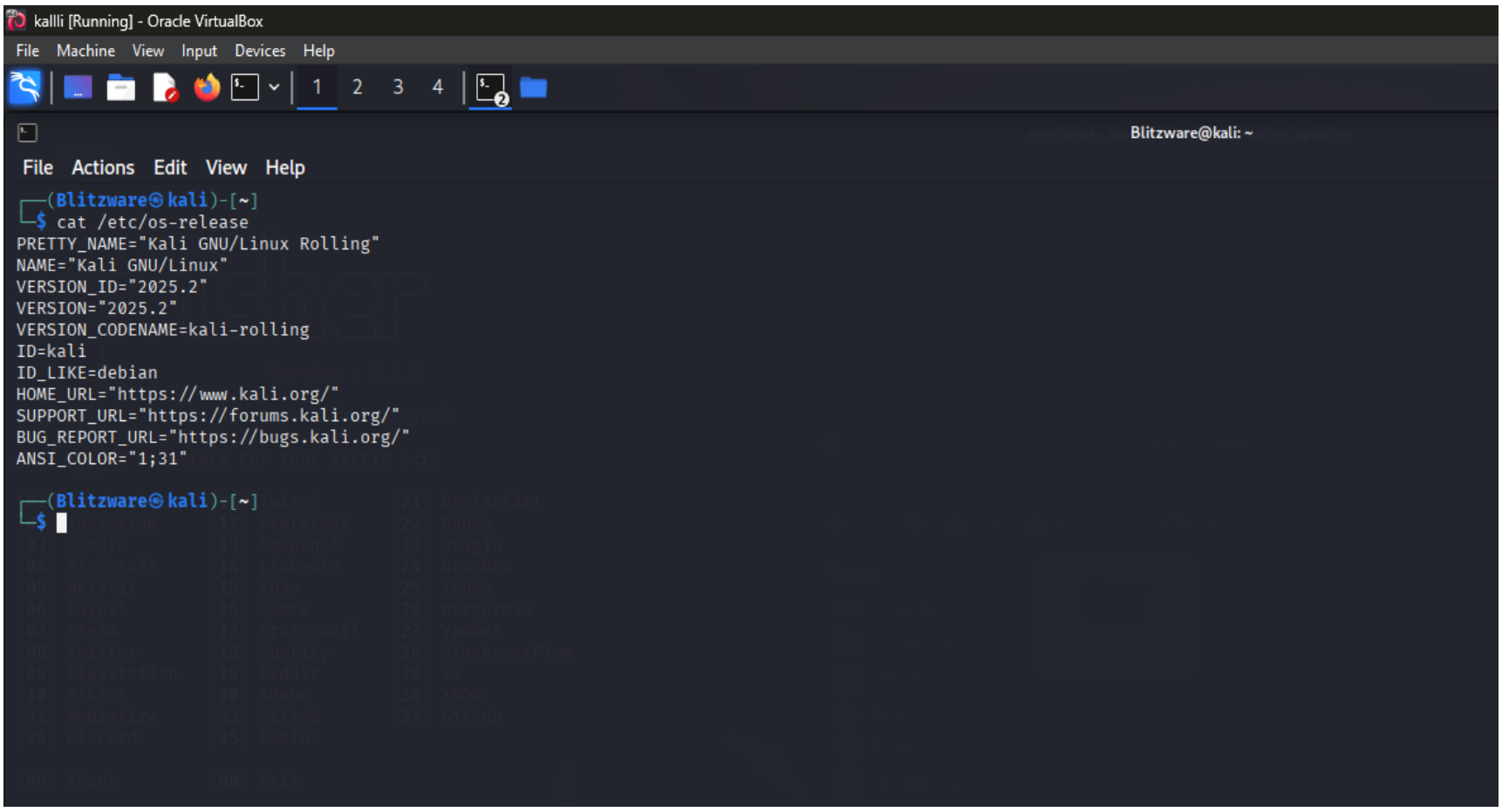
This hands-on simulation helped in exploring the workflow of phishing attacks, learning how phishing pages are hosted, and observing how unsuspecting users could fall for such traps.

Lab Setup

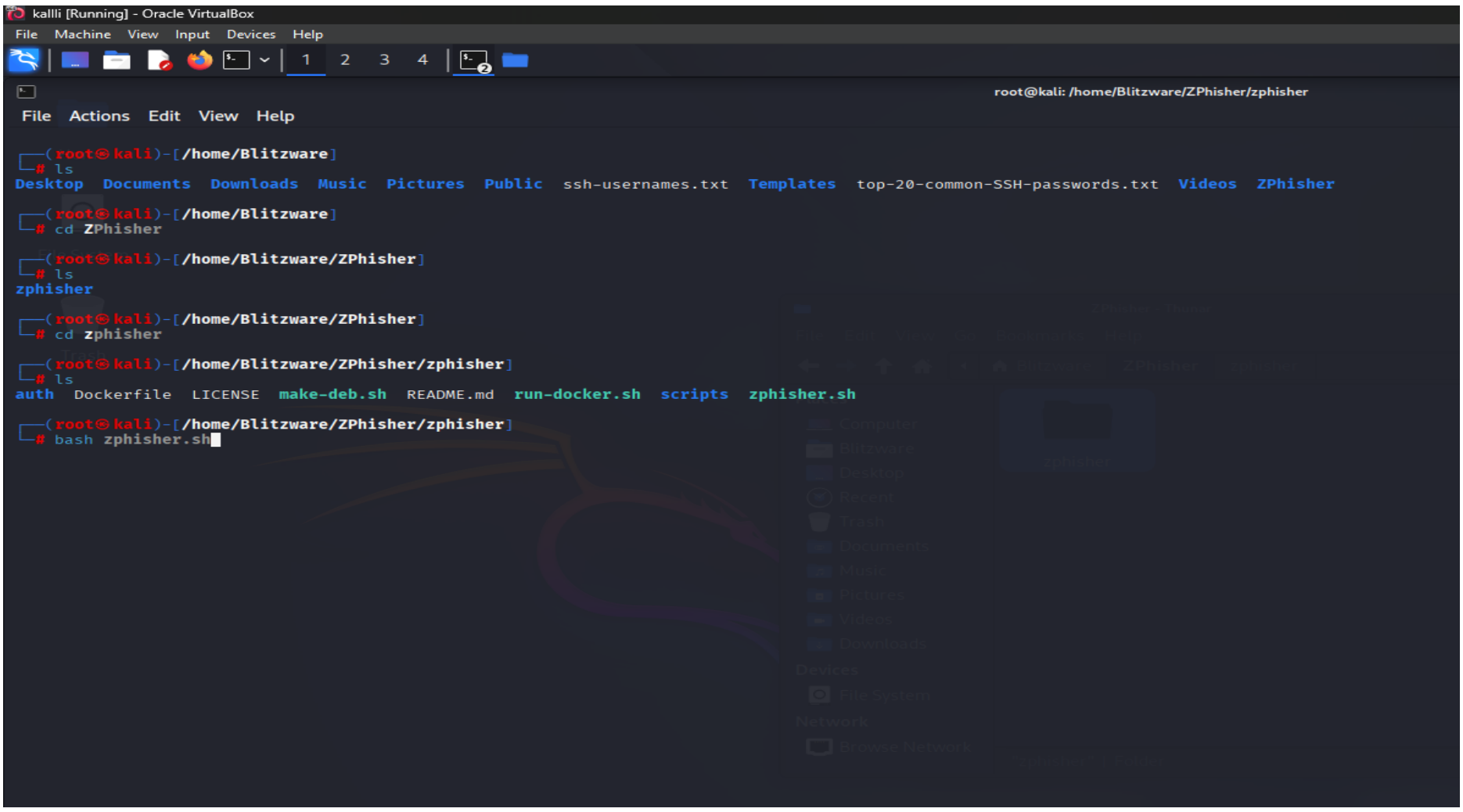
Component	Description
Host Machine	Kali Linux (running in VirtualBox)
Network Mode	Bridge Adapter (for proper tunnel access)
Phishing Tool	Zphisher (a social engineering toolkit)
Targeted Services	LinkedIn, Facebook
Tunnelling Services	Cloudflare (auto-generated by Zphisher)
Note	No real victim was involved. This was strictly for ethical and educational purposes.

Execution Steps

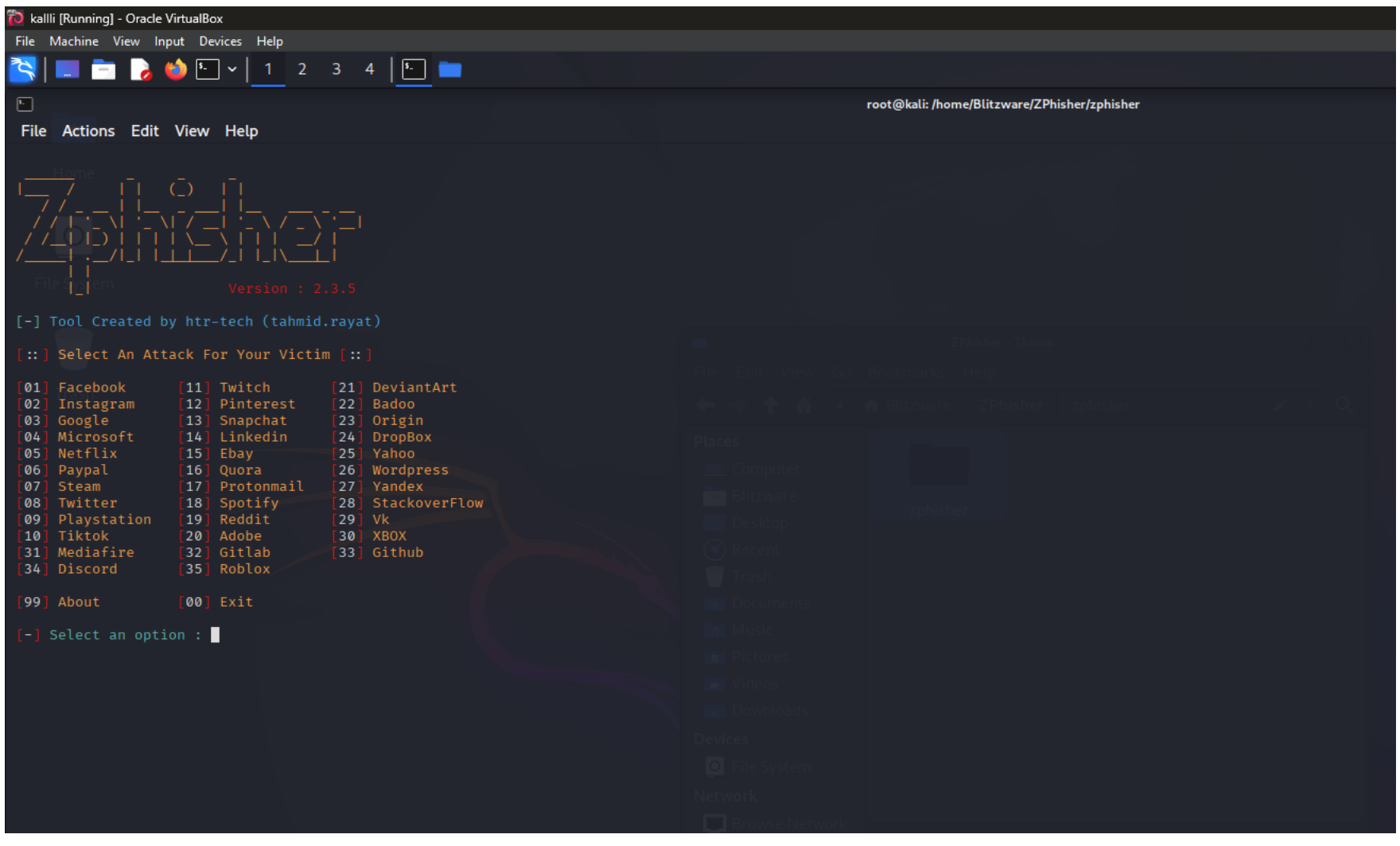
- Kali Linux was launched, and its version was verified for compatibility.



- A dedicated directory was created: /Zphisher.
- Zphisher was cloned and configured from its GitHub repository: https://github.com/htr-tech/zphisher
- The tool was executed via terminal using: bash zphisher.sh



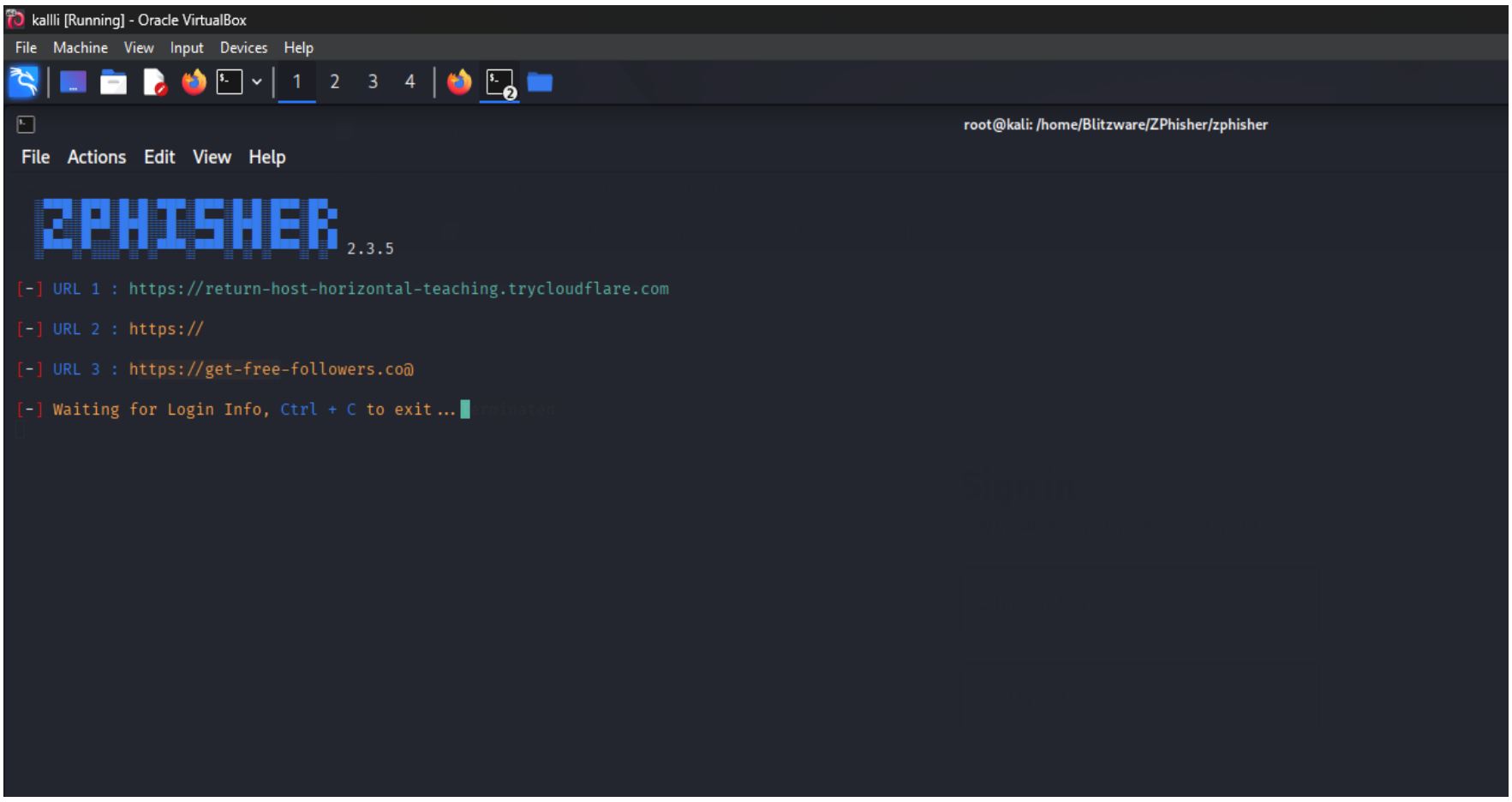
- The tool presented multiple platforms for phishing simulation. LinkedIn was selected first, followed by Facebook.

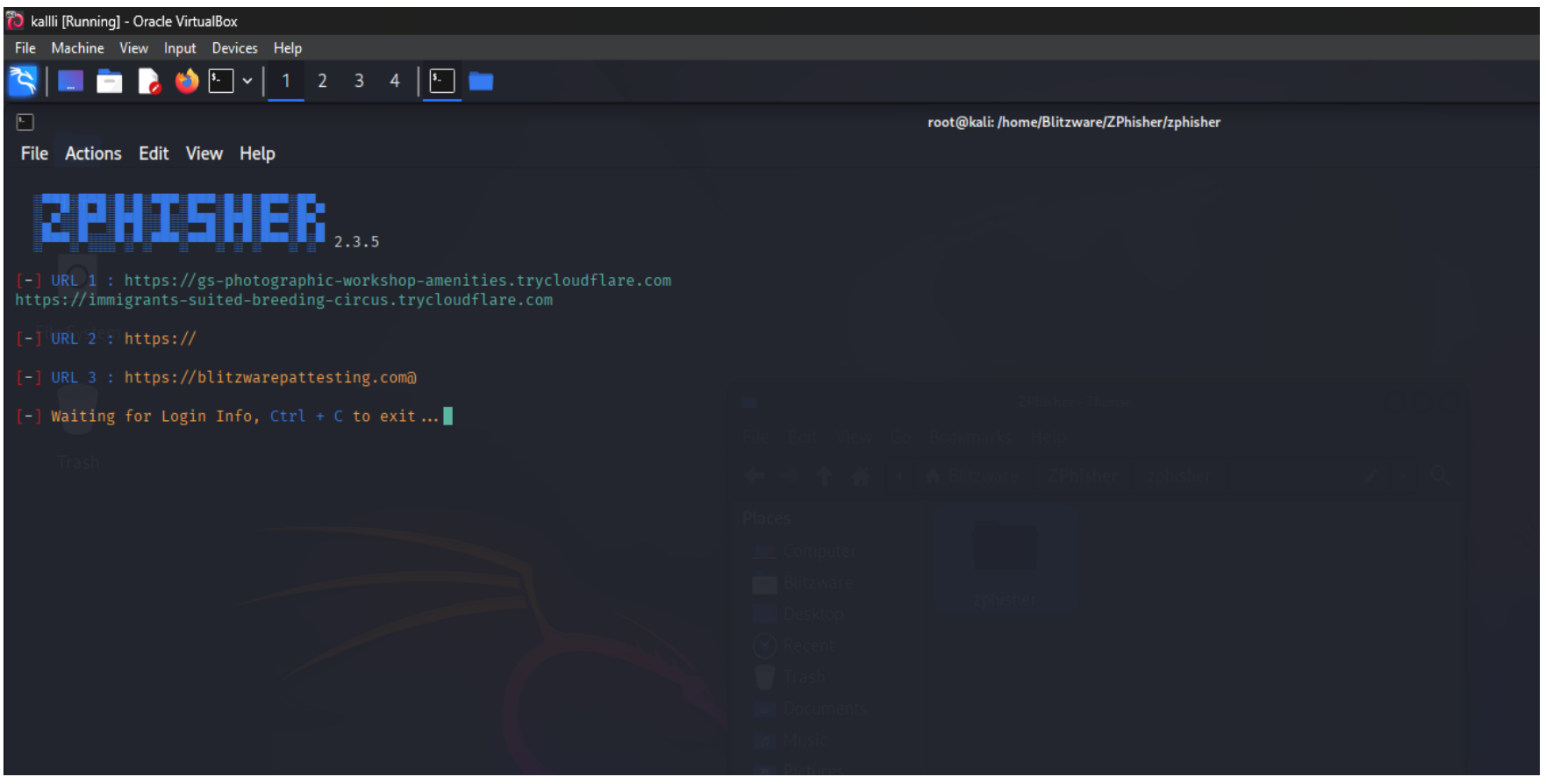


- Upon selecting a target, Zphisher generated multiple phishing URLs using tunneling options:
  - Localhost

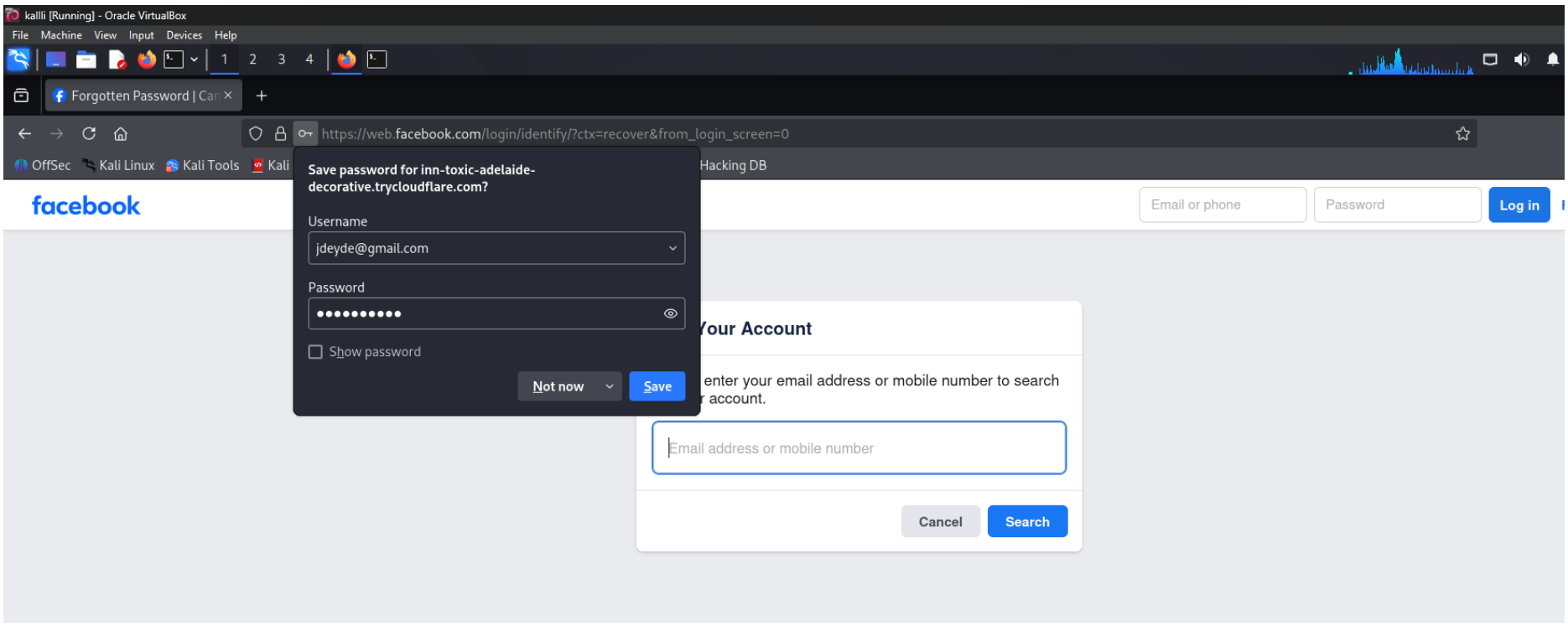
- Cloudflare

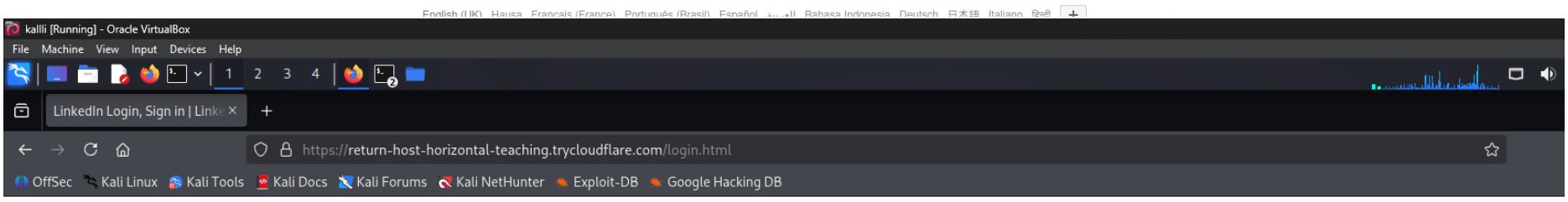
- URLs were generated that could be used to access both the masked page to carry out the phishing.

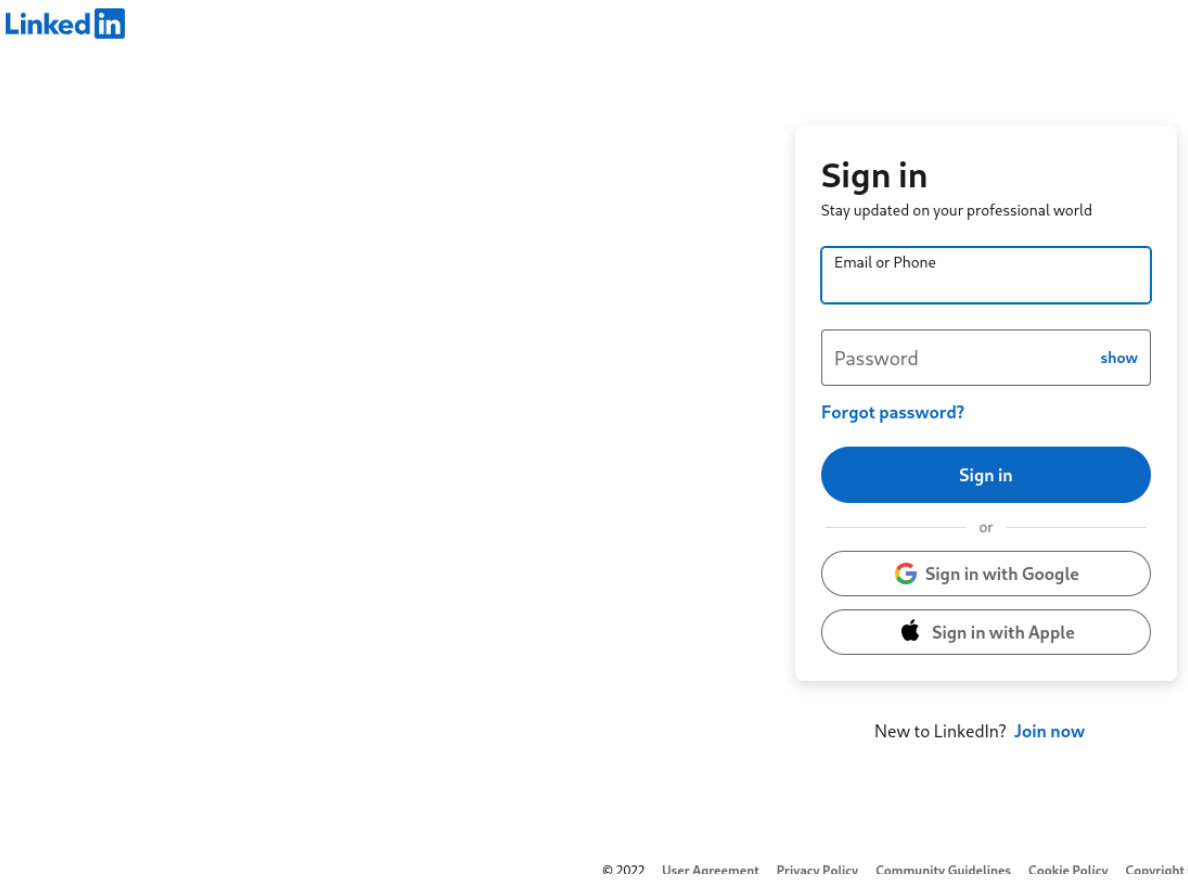




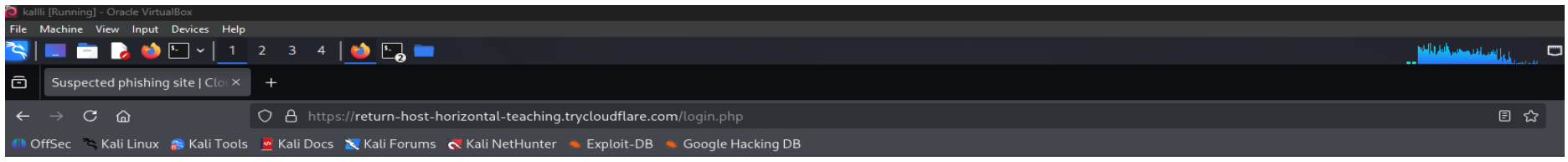
- The Cloudflare URL was successful it hosted a fake login page of both LinkedIn and Facebook.



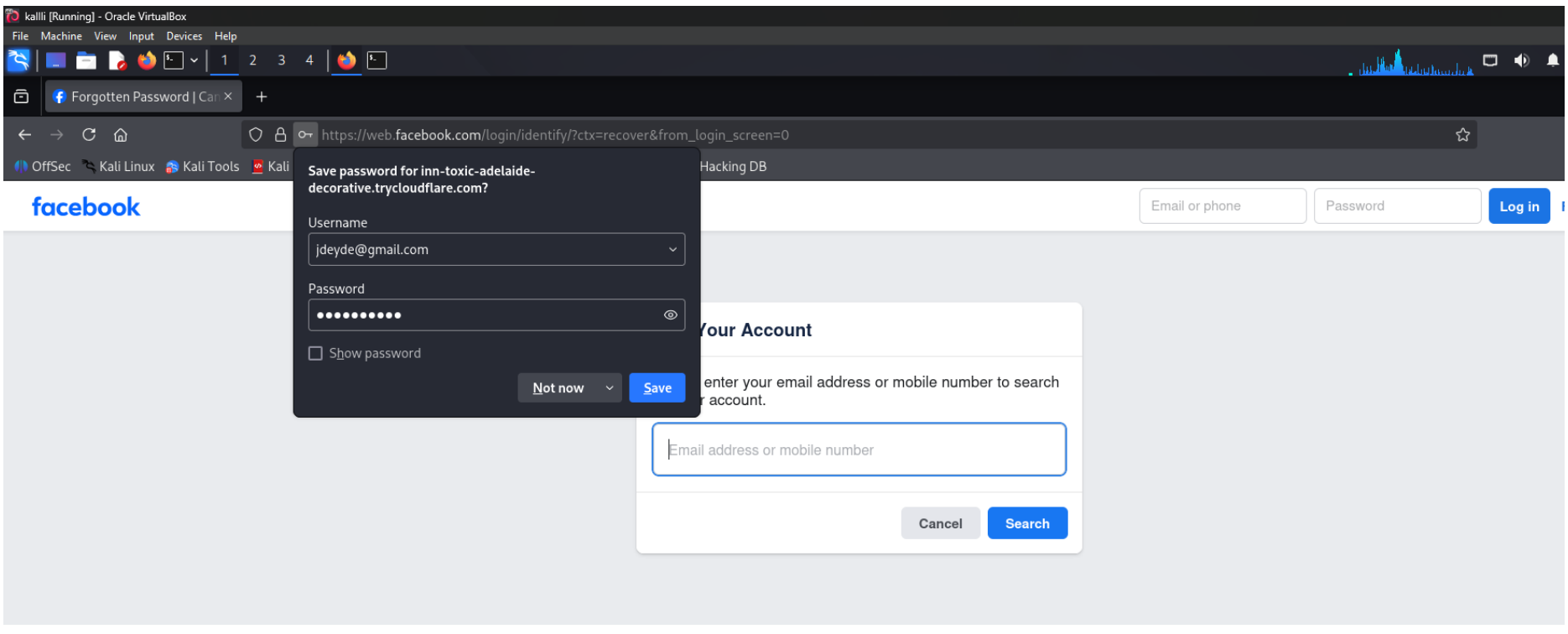




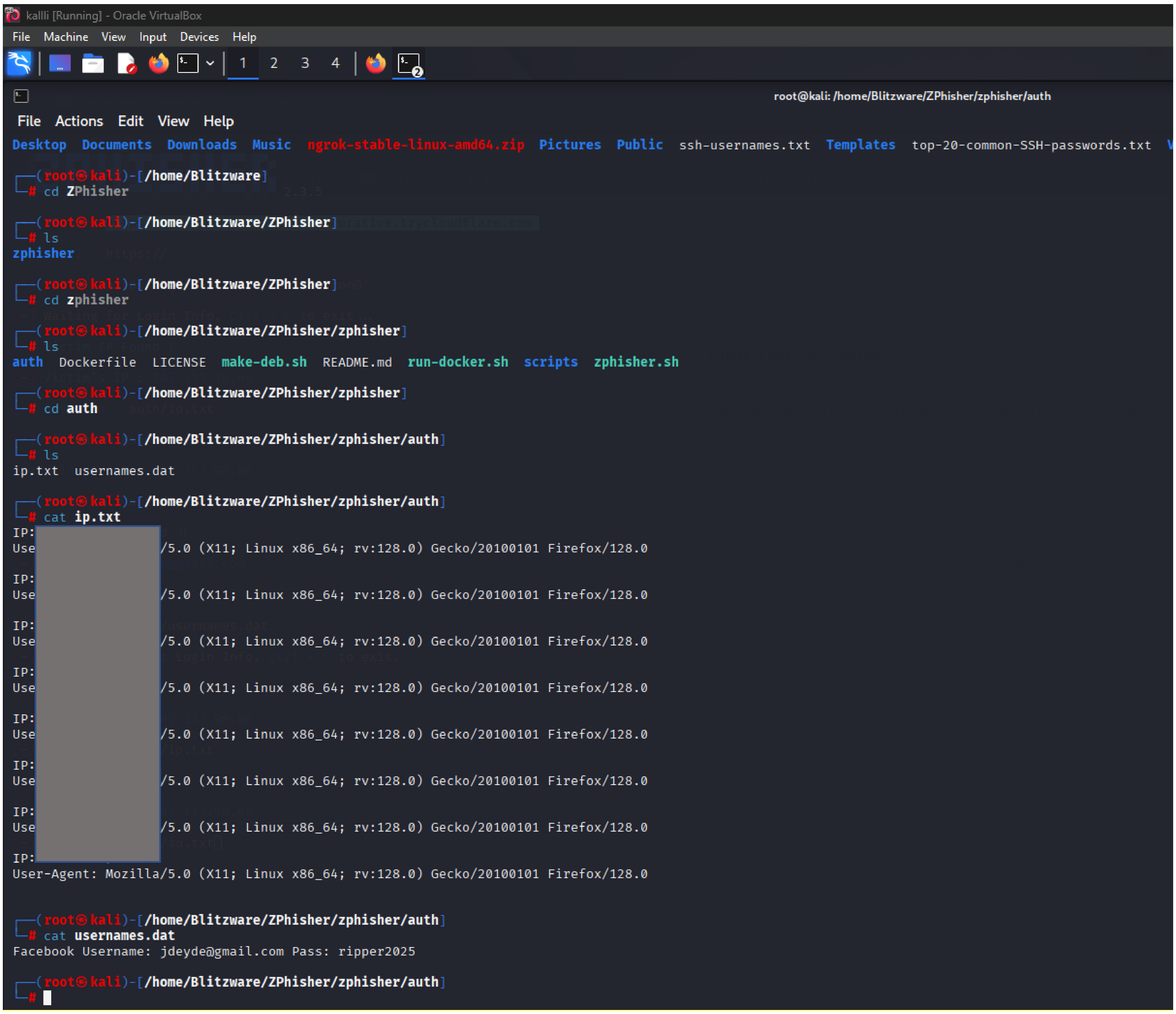
- When the LinkedIn phishing page was accessed, the browser flagged it as a suspected phishing site and blocked access.



- The Facebook phishing page was able to bypass the warning, load successfully, and capture data.



- Upon submission of dummy login credentials, the entered username was successfully captured and stored inside the auth folder on the attacking machine.



Issues Encountered

- Not all the generated phishing links were functional. Only the Cloudflare-based tunnel link successfully hosted the phishing page.
- The browser's security system detected and blocked the LinkedIn phishing page, showcasing real-world browser defence mechanisms.

Ethical Consideration

This phishing simulation was conducted solely for educational and ethical learning purposes.

No real users were targeted, and all tests were done within a closed lab environment to practice and understand adversarial techniques in a safe and responsible manner.

Next Steps & Recommendations

Explore defensive countermeasures, such as:

- Browser hardening
- Deploying Intrusion Detection Systems (IDS/IPS)
- Conducting phishing awareness training simulations

- Extend the lab to include email phishing simulations and payload delivery testing in a sandbox environment.

Conclusion

This simulation demonstrated how attackers can use open-source phishing kits like Zphisher to exploit user trust by mimicking familiar login pages. It also highlighted the importance of:

- Browser based phishing detection systems
- Network security awareness
- The role of tunnelling in bypassing local restrictions

Further exercises can involve defensive testing, such as setting up IDS/IPS, browser security hardening, or simulating phishing awareness responses.